IN THE CLAIMS:

1. (Previously Presented) A method for packet bypass in a communications network with an asymmetrical upstream and downstream transmission rate, comprising:

receiving a plurality of packets;

determining whether each packet is a bypass packet or a non-bypass packet;

optimally selecting a maximum number of bypass packets to communicate between two non-bypass packets to maximize the downstream transmission rate without substantially interfering with the upstream transmission rate;

communicating the non-bypass packets toward a communication link; and

communicating a plurality of the bypass packets toward the communication link between communication of two of the non-bypass packets,

wherein each bypass packet comprises an acknowledgment message, and

wherein each bypass packet comprises a Transmission Control Protocol (TCP) packet containing an acknowledgment message.

2. (Canceled)

3. (Original) The method of Claim 1, wherein determining whether each packet is a bypass packet or a non-bypass packet comprises determining a size of the packet.

4. (Original) The method of Claim 3, wherein determining the size of the packet comprises classifying packets having a size smaller than a specified size as bypass packets.

5. (Original) The method of Claim 1, wherein determining whether each packet is a bypass packet or a non-bypass packet comprises determining a content of the packet.

6. (Canceled)

7. (Original) The method of Claim 1, wherein determining whether each packet is a bypass packet or a non-bypass packet comprises determining at least one of a size of the packet, a protocol used to generate the packet, and a content of the packet.

8. (Previously Presented) A method for packet bypass in a communications network, comprising:

receiving a plurality of packets;

determining whether each packet is a bypass packet or a non-bypass packet;

communicating the non-bypass packets toward a communication link; and

communicating a plurality of the bypass packets toward the communication link between communication of two of the non-bypass packets,

wherein determining whether each packet is a bypass packet or a non-bypass packet comprises:

determining a size of the packet;

if the packet does not have a specified size, classifying the packet as a non-bypass packet, otherwise determining a protocol used to generate the packet;

if the packet was not generated using a specified protocol, classifying the packet as a non-bypass packet, otherwise determining a content of the packet; and

if the packet does not include at least a portion of a specified content, classifying the packet as a non-bypass packet, otherwise classifying the packet as a bypass packet.

9. (Original) The method of Claim 1, further comprising determining a maximum number of bypass packets that can be communicated between communication of two of the non-bypass packets.

10. (Original) The method of Claim 1, further comprising storing each bypass packet and each non-bypass packet in a memory wherein the bypass packets and non-bypass packets can be selectively retrieved from the memory.

11. (Original) The method of Claim 10, wherein the memory comprises:

a bypass memory operable to store bypass packets; and

a transmit memory separate from the bypass memory and operable to store non-bypass packets.

12. (Previously Presented) The method of Claim 1, wherein the communication link comprises an Asymmetrical Digital Subscriber Line residing between a modem and a central office switch.

13. (Original) The method of Claim 1, wherein the communication link comprises at least one of a universal serial bus, a Peripheral Component Interconnect local bus, or an Ethernet connection, residing between a host and a modem.

14. (Previously Presented) A system for packet bypass in a communications network having an asymmetrical communications link with an upstream and downstream bandwidth with different sizes, comprising:

at least one computer readable medium; and

software encoded on the computer readable medium, the software operable when executed to:

receive a plurality of Transmission Control Protocol (TCP) packets;

determine whether each packet is a bypass packet or a non-bypass packet;

communicate the non-bypass packets upstream toward the asymmetrical a communication link; and

communicate a plurality of the bypass packets upstream toward the asymmetrical communication link between communication of two of the non-bypass packets,

wherein the software is operable to communicate up to a specified maximum number of bypass packets between communication of two non-bypass packets and wherein the maximum number is optimally selected to maximize the downstream bandwidth.

15. (Original) The system of Claim 14, wherein each bypass packet comprises an acknowledgment message.

16. (Original) The system of Claim 14, wherein the software is operable to determine whether each packet is a bypass packet or a non-bypass packet by determining a size of the packet.

17. (Original) The system of Claim 16, wherein determining the size of the packet comprises classifying packets having a size smaller than a specified size as bypass packets.

18. (Original) The system of Claim 14, wherein the software is operable to determine whether each packet is a bypass packet or a non-bypass packet by determining a content of the packet.

19. (Canceled)

20. (Original) The system of Claim 14, wherein the software is operable to determine whether each packet is a bypass packet or a non-bypass packet by determining at least one of a size of the packet, a protocol used to generate the packet, and a content of the packet.

21. (Original) The system of Claim 14, wherein the software is operable to determine whether each packet is a bypass packet or a non-bypass packet by:

determining a size of the packet;

if the packet does not have a specified size, classifying the packet as a non-bypass packet, otherwise determining a protocol used to generate the packet;

if the packet was not generated using a specified protocol, classifying the packet as a non-bypass packet, otherwise determining a content of the packet; and

if the packet does not include at least a portion of a specified content, classifying the packet as a non-bypass packet, otherwise classifying the packet as a bypass packet.

22. (Canceled)

23. (Original) The system of Claim 14, wherein the software is further operable to store each bypass packet and each non bypass packet in a memory wherein the bypass packets and non-bypass packets can be selectively retrieved from the memory.

24. (Original) The method of Claim 23, wherein the memory comprises:

a bypass memory operable to store bypass packets; and

a transmit memory separate from the bypass memory and operable to store non-bypass packets.

25. (Original) The system of Claim 14, wherein the communication link comprises an Asymmetrical Digital Subscriber Line residing between a modem and a central office switch.

26. (Original) The system of Claim 14, wherein the communication link comprises at least one of a universal serial bus, a Peripheral Component Interconnect local bus, or an Ethernet connection, and resides between a host and a modem.

27. (Canceled)

28. (Canceled)

29. (Currently Amended) ~~The system of Claim 27~~ A system for packet bypass in a communications network having an asymmetrical communications link with an upstream and downstream bandwidth that are different sizes, comprising:

a communications manager operable to receive a plurality Transmission Control Protocol (TCP) packets and to determine whether each packet is a bypass packet or a non-bypass packet; and

a memory accessible to the communications manager and operable to receive bypass packets and non-bypass packets from the communications manager;

wherein the communications manager is further operable to retrieve bypass packets and non-bypass packets from the memory and to communicate upstream toward the asymmetrical communication link a plurality of the bypass packets between communication of two of the non-bypass packets,

wherein the downstream bandwidth is larger than the upstream bandwidth, and

wherein the communications manager is operable to communicate up to a specified maximum number of bypass packets between communication of two non-bypass packets,

wherein the communications manager is operable to determine whether each packet is a bypass packet or a non-bypass packet by determining a size of the packet.

30. (Original) The system of Claim 29, wherein the communications manager is operable to classify all packets having a size smaller than a specified size as bypass packets.

31. (Canceled)

32. (Canceled)

33. (Canceled)

34. (Currently Amended) ~~The system of Claim 27~~ A system for packet bypass in a communications network having an asymmetrical communications link with an upstream and downstream bandwidth that are different sizes, comprising:

a communications manager operable to receive a plurality Transmission Control Protocol (TCP) packets and to determine whether each packet is a bypass packet or a non-bypass packet; and

a memory accessible to the communications manager and operable to receive bypass packets and non-bypass packets from the communications manager;

wherein the communications manager is further operable to retrieve bypass packets and non-bypass packets from the memory and to communicate upstream toward the asymmetrical communication link a plurality of the bypass packets between communication of two of the non-bypass packets,

wherein the downstream bandwidth is larger than the upstream bandwidth, and

wherein the communications manager is operable to communicate up to a specified maximum number of bypass packets between communication of two non-bypass packets,

wherein the communications manager is operable to determine whether each packet is a bypass packet or a non-bypass packet by:

determining a size of the packet;

if the packet does not have a specified size, classifying the packet as a non-bypass packet, otherwise determining a protocol used to generate the packet;

if the packet was not generated using a specified protocol, classifying the packet as a non-bypass packet, otherwise determining a content of the packet; and

if the packet does not include at least a portion of a specified content, classifying the packet as a non-bypass packet, otherwise classifying the packet as a bypass packet.

35. (Canceled)

36. (Canceled)

37. (Currently Amended) ~~The system of Claim 27~~ A system for packet bypass in a communications network having an asymmetrical communications link with an upstream and downstream bandwidth that are different sizes, comprising:

a communications manager operable to receive a plurality Transmission Control Protocol (TCP) packets and to determine whether each packet is a bypass packet or a non-bypass packet; and

a memory accessible to the communications manager and operable to receive bypass packets and non-bypass packets from the communications manager;

wherein the communications manager is further operable to retrieve bypass packets and non-bypass packets from the memory and to communicate upstream toward the asymmetrical communication link a plurality of the bypass packets between communication of two of the non-bypass packets,

wherein the downstream bandwidth is larger than the upstream bandwidth, and

wherein the communications manager is operable to communicate up to a specified maximum number of bypass packets between communication of two non-bypass packets,

wherein at least a portion of the communications manager resides within a modem coupled to a host computer.

38. (Original) The system of Claim 37, wherein the modem comprises an external modem coupled to the host computer.

39. (Currently Amended) ~~The system of Claim 27~~ A system for packet bypass in a communications network having an asymmetrical communications link with an upstream and downstream bandwidth that are different sizes, comprising:

a communications manager operable to receive a plurality Transmission Control Protocol (TCP) packets and to determine whether each packet is a bypass packet or a non-bypass packet; and

a memory accessible to the communications manager and operable to receive bypass packets and non-bypass packets from the communications manager;

wherein the communications manager is further operable to retrieve bypass packets and non-bypass packets from the memory and to communicate upstream toward the asymmetrical communication link a plurality of the bypass packets between communication of two of the non-bypass packets,

wherein the downstream bandwidth is larger than the upstream bandwidth, and

wherein the communications manager is operable to communicate up to a specified maximum number of bypass packets between communication of two non-bypass packets,

wherein at least a portion of the communications manager resides within a host computer.